General Order 93.06 - 02/19/02
Facial Recognition Utilization/Procedures

Purpose:

The Virginia Beach Police Department is committed to the safety and security of the citizens and visitors of Virginia Beach. To ensure this commitment, the Virginia Beach Police Department constantly strives to research and utilize the latest technology to enhance the performance of departmental members. To that end, the Department is enhancing its current video technology capabilities with the introduction of Biometrics in the form of facial recognition technology.

Definition:

1. Biometrics - Automated methods of recognizing and identifying a person based on physiological or behavioral characteristics such as fingerprinting, voice patterns, or facial recognition.

2. Facial Recognition Technology - The automated process of converting an image or photo into a mathematical, computer algorithm as a basis for recognition and potential identification. The software creates a digital map of an individual's face by translating the contours into mathematical formulas that are nearly as distinguishable as fingerprints.

Procedures:

1. Database:

A photographic database of wanted criminals with outstanding felony warrants, or certain misdemeanors that involve violence (i.e., assaults, etc.), reported missing persons, and reported runaways, will be created using photographs of those persons meeting the above criteria. The database may include persons meeting this criteria wanted by law enforcement agencies other than the Virginia Beach Police Department. Additionally, photographs of department personnel, city leaders, or citizen volunteers may be entered into the system with their permission to serve as a verification system. This database will be utilized with the Facial Recognition Technology (FRT) and the Oceanfront CCTV camera systems.

Personal images, with a minimum threshold of 14 match points, captured by the camera system will be compared to those in the database. Those individual images found to match a wanted person, runaway or missing person, or test subjects will be maintained until such time that the image no longer meets the above stated criteria. All other individual images will be immediately discarded.

2. Alert Procedures:

When the Camera Monitoring Officer (CMO) receives an alert of a possible hit, he will view the two (2) photographs displayed to confirm that the software has identified a subject within the database. The CMO shall maintain a CMO Monitor's Log that will be utilized to document any alerts that may be registered by the FRT system. This will include all hits, encounters and the final disposition of any encounters. In addition to this log, the CMO shall also complete a FRT Hit form in the event positive identification and an arrest is made based on the technology.

Upon visually confirming the photograph is a possible match, the CMO will determine the nature of the alert (i.e., wanted person, runaway, or missing person). Based on the nature of the alert, the CMO will simultaneously contact the nearest patrol officer and an On Duty First Line Supervisor and advise of the potential hit and the nature of the alert. Upon this notification the CMO shall implement the appropriate responses depicted as follows:

A. Wanted Persons - After confirming the hit, the CMO will notify the closest uniformed officers of the alert, description of the subject, the specific charges, and the direction of travel. The CMO will then immediately confirm the existence and location of the warrant/s. After confirming the existence and location of the warrant/s, the CMO will notify the responding officers of that information. While confirming the warrant/s, the CMO will also obtain any additional information that may assist responding officers and ensure their safety, the safety of the subject to be encountered, as well as any bystanders.

The responding officers will locate and approach the possible subject based on Reasonable Suspicion, and conduct an "investigatory" stop (Terry v Ohio). It is imperative that the officers remember that this encounter is for investigative purposes only and that the alert or hit with the FRT is not probable cause for an arrest. At the earliest opportunity, the officer(s) will provide the citizen with an explanation of why they were stopped.

The officer(s) will take the necessary investigative steps to determine if the subject is in fact wanted. If the officer(s) determine that the subject of their encounter is not wanted he will be given a brief explanation for the encounter and immediately released. If the subject is confirmed as being wanted, the subject will be immediately taken into custody in accordance with existing policy and procedures. The officers shall immediately notify a supervisor and the CMO of the final disposition of the encounter and the actions that were taken.

The arresting officers shall process the prisoner in accordance to existing policy and procedures and they shall fax a copy of the tracer report to the CMO for documentation purposes. The CMO shall complete a FRT Hit form documenting the encounter and arrest.

B. Runaways - After confirming the hit, the CMO will confirm the status of the runaway

through NCIC and/or PISTOL. The CMO will also contact Juvenile Intake and confirm the existence of an active pick up order. The CMO will also request any additional information from the Intake worker that may assist and ensure the safety of the responding officers, bystanders, and the juvenile to be encountered.

The officers will approach the juvenile and using an investigatory stop, determine if the juvenile is in fact the runaway. If the juvenile is not the runaway and if there are no other underlying reason or causes for detention (curfew, etc.), the juvenile will be given a brief explanation for the encounter and released. If the juvenile is determined to be the runaway, they will be taken into custody in accordance with existing policies and procedures and transported to juvenile intake. The CMO and supervisor will be notified of the final disposition of the encounter. The CMO will document the encounter as described above with due regard to the juvenile status of the offender.

C.   Missing Persons - The same procedures shall apply with the identifying and encounters of a missing person. The CMO after confirming the hit shall attempt to confirm the IBR (Incident Based Reporting) for missing persons and any other information such as medical condition or other factors. The responding officers shall conduct an investigatory stop to determine the identity of the subject and take the appropriate action. If the person approached is not the missing person, they will be given a brief explanation for the encounter and released. The supervisor and CMO will be notified of the final disposition of the encounter.

D.   Federal Bureau of Investigation Terrorist Most Wanted List - The FBI maintains a list of subjects that are wanted for questioning or have active federal warrants on file, regarding terrorist activities and/or threats. Images of individuals on this list will be entered into the database with the appropriate FBI alerts and contact numbers. The CMO will check with the FBI on a daily basis to determine status of the individuals on the list and remove or enter images as required by this policy.

E.   External Digitized Images - The Virginia Beach Police Department currently utilizes digital technology to capture digital video and still images by use of handheld video and still cameras. The use of this technology allows for more mobility, which furthers the capabilities of the Facial Recognition Technology. In the event that a subject meeting the criteria outlined in this policy is located outside of the viewing area of the fixed FRT cameras, their digital image may be captured by handheld digital recording devices and entered into the database for processing. If an alert is received, the proper response outlined in this policy will be implemented. In the event that there is no alert, the image will be immediately removed from both the FRT system as well as the recording media used to capture the image. The use and input of external digital images will only be utilized with the approval of the Commanding Officer of the Second Police Precinct or the Commanding Officer of Special Investigations, or their designees.

Random external digitized images of persons and/or crowds will not be entered into the FRT, for any reason. A request for use of the FRT with external digital images, will be noted in the FRT log with the specific reason for the request. In addition, the CMO will complete the FRT Alert form.

3.   CMO Alert/Encounter Logs:

The CMO will maintain a log for documenting all alerts and encounters that are a direct result of the FRT System. These logs will be reviewed on a weekly basis by the Second Precinct Lieutenant who shall submit a monthly report to the Chief of Police via the Chain of Command. These logs shall be maintained at the Second Police Precinct for three (3) years and shall be disposed of, in accordance with existing policies and procedures.

4.   Systems Operation:

Under normal operations criteria, the CMO will ensure that the Facial Recognition System is operating in its automatic mode and receiving inputs from the two dedicated cameras. The CMO will not manually cause the system to target any individuals unless they are searching for a wanted person who has been specifically identified by citizens, a law enforcement officer, or other verifiable means, or missing persons who have been reported by citizens and/or police officers.

Under no circumstances will members of the CMO or any other Department member allow the system to be operated in a manner that could be construed or perceived as being discriminatory towards anyone based on race, gender, ethnicity, or any other non-criminal criteria.

5.   Security:

There will be multiple layers of security, which prohibit unauthorized entry or removal of information from the database. Only sworn police officers specifically identified and authorized in writing by the Chief of Police shall have access to the database. The identified officers will have the sole responsibility for entering images into the database and ensuring that all those in the database meet the governing criteria on an ongoing basis. This will require constant verification of warrants and other investigative reporting for runaways and missing persons.

The system will also be password protected with only authorized officers possessing the password. As an additional level of security, the password will be changed at least every 180 days by the system administrator.

Finally, to ensure no unauthorized entry into the database, the system will be a stand-alone system and not connected to any LAN/WAN. Information in the database will not be shared with anyone without the expressed approval of the Chief of Police.

6.   Entry/Validation:

The CMO will receive a daily report from Police Services listing all new felony warrants issued. After receiving the listing, the CMO will coordinate with Forensic Services Unit and/or the Sheriff's Department Central Booking Unit to determine if a photograph of the subject is available. If a photograph is available, it will be requested and entered into the system after the CMO ensures it meets all applicable criteria.

To ensure current and accurate data, the CMO will also receive a report daily from Police Services detailing the warrants served for the previous 24 hours. The CMO will compare the warrants served with the database to ensure that images of those individuals arrested are removed.

7.   Audit:

The precinct lieutenant responsible for camera operations will conduct quarterly audits to ensure all policies and procedures concerning the Facial Recognition Technology System is functioning properly. A report of this audit will be provided to the Chief of Police and maintained in the grant documentation.

Additionally, random audits will be conducted by the Facial Recognition Program Citizen Advisory and Audit Committee. Between the dates of May 1st and September 30th, the Committee will conduct monthly audits. During the remaining months between October 1st and April 30th, the Committee will conduct quarterly audits. Committee members will have complete and open access to databases, alert/encounter logs, and any other documentation pertaining to the facial recognition program.

Members of the audit committee will provide a written report utilizing the Facial Recognition Audit Form outlining their findings, assessment, and recommendations to the Chief of Police within 48 hours of any audit/review they conduct. Copies of these reports will be maintained with other grant documentation and utilized during the ongoing evaluation process.

Facial Recognition Alert and Encounter Report

Date of Alert:	Time of Alert:
CMO Name and Code:	Supervisor Notified:
System Verification Alert: ___ Yes ___ No	Test Officer Name/Code:

Nature of Alert: ___ Wanted Persons ___ Runaway ___ Missing Person
If Warrant: ___ Felony ___ Misdemeanor
Specific Charges:

Additional Information/Caution Indicators:

Alert Verification: _____ Yes _____ No (If no, reason):	
Warrant/Pickup Order Confirmed: Y N	Clerks Name:

Name and Code of Officers Notified:

Date of Encounter:	Time of Encounter:

Location of Encounter:

Problems with Encounter (if any):

Final Disposition of Encounter: ____ Arrest ___ Released	
Arrest Direct Result of FRT: ___ Yes ___ No	Additional Charges (if any):

If No, What was arrest based on?:

Miscellaneous Information:

CMO Signature:	Date and Time:
Lieutenants Signature:	Date and Time:

Facial Recognition Alert/Encounter Logbook							
Date	Time	Alert Type	Location	Supervisor Code	Officers Code	Final Disposition	CMO Code

M E M O R A N D U M

To: Chief of Police A.M. Jacocks Jr.

From: Facial Recognition Committee Members:_____

Date: _____

Subject: Facial Recognition Technology Audit

Facial Recognition Audit Form	
Date and Time of Audit:	
Name of CMO/Code:	Supervisor/Code:
Name of Auditor:	Second Auditor:
FR Alert and Encounter Reports Inspected: _____ Yes _____ No	
Comments:	
FR Alert and Encounter Logbook Inspected: _____ Yes _____ No	
Comments:	

Database Integrity/Security Within Policy: _____ Yes _____ No	
Comments:	
Facility Security Within Policy: _____ Yes _____ No	
Number of Random Pulls: # _____	Number of Verifications: # _____
Comments, Suggestions, and/or Recommendations:	
Signatures:_____ Date: _____	

*Forward a copy to the Second Precinct FRT Coordinator